

INTERVIEW:

Det Supt Ian Kirby: ‘Every cop should have the basic knowledge to go out there and support a victim’

OPEN

12th January 2024
James Sweetland, Policing Insight

In the second part of his interview with Policing Insight, Det Supt Ian Kirby, the recently appointed CEO of the National Cyber Resilience Centre Group, spoke to James Sweetland about the benefits of the Cyber PATH programme, and the importance of all officers having enough understanding of cybercrime to be able to offer basic advice and support to victims.

In the second part of Policing Insight's conversation with Det Supt Ian Kirby, the recently appointed CEO of the National Cyber Resilience Centre Group (NCRCG), we turned first to the Cyber PATH programme run by the NCRCG.

This innovative scheme puts students at the heart of the Group's work, building a workforce for the future while supporting efforts to boost the cybersecurity of small businesses.

Det Supt Kirby's enthusiasm for Cyber PATH is clear: "It's really important that we talk about this programme that's creating this workplace-ready talent pipeline, because it has multiple benefits. And for me personally, it goes back to that 'helping the person cross the road' feeling, that sense of public service that's so powerful."

So, what is Cyber PATH and how does it work? "I engage with 42 universities across England and Wales to recruit our students – and they're not just going to be doing work experience, that's a misconception.

"We run the recruitment process through the summer, open to everybody on computer science and cybersecurity type courses. Those who are successful during the recruitment are employed as Cyber PATH students; they become employees of the NCRCG, and we use them to deliver technical services to our small and medium business clients.

"Our regional centres, which are the shopfront for providing technical services, agree a price with the clients. I then direct my students to deliver those services under the watchful eye of two qualified technical supervisors, and a qualified technical senior who signs off on all their work. All the students are client-facing from day one; they engage with the client and scope what service they deliver."

The scheme is all about providing small and medium-sized enterprises (SMEs) with understandable advice that can help them protect themselves from cybercrime, said Det Supt Kirby.

"They will deliver the service and write the technical report but, importantly, write in a way which is simple to understand. Many cybersecurity providers will write a highly technical report and then deliver it to maybe a chief security officer at a large company.

“If you’re an SME, perhaps a plumber’s merchant, you haven’t got the benefit [of many IT staff.] You need to be given a report that’s digestible and easy to understand.”

The scheme also offers a remarkable professional development opportunity, especially as the NCRCG’s private sector ‘ambassadors’ provide extra interview and CV advice training to the students.

“They build their people skills by being client-facing, and get a well-rounded sense of what interviewers are looking for. When they leave our programme, finish their degree and start on their first job interviews, they are absolutely head and shoulders above their peers. They walk straight into some really powerful jobs, both within law enforcement and other agencies and organisations.”

A recent Department for Science, Innovation and Technology (DSIT) report found that the UK’s cybersecurity workforce isn’t sufficient to meet the demand for cyber skills, so efforts to build this ‘workplace-ready talent’ could prove vital, especially given the challenges some firms have faced.

As Det Supt Kirby explained: “One of my national ambassadors mentioned that he spent tens of thousands of pounds recruiting a load of new graduates and he had to let them all go because none of them could speak to people.

“None of them had ever been client-facing and he couldn’t put them in front of clients. But with Cyber PATH, we’re producing a really well-rounded individual [who has those skills.]”

There are some success stories with Cyber PATH. The programme is currently developing more than 50 students, while a recent recruitment campaign for the next round attracted over 100 applications.

Recent graduates from the scheme have gone on to jobs at Siemens, Cyberfort, the DSIT, as well as within law enforcement and policing. One former Cyber PATH student, Sophie Powell (a Warwick University cyber security graduate), worked with the West Midlands Cyber Resilience Centre during her time on the programme, and was later named Cyber Student of the Year at the National Cyber Awards 2023.

With 226 technical services delivered across the regional cyber resilience centres by Cyber PATH students last year, the hope is that a growing pipeline can be one of the main achievements of the NCRCG.

The cyber threat landscape

Alongside programmes like Cyber PATH, part of the NCRCG's role is to help spread awareness of the cybercrime and fraud threats facing SMEs. According to *Cracking the case: uncovering the cost of small business crime*, a December 2023 report from the Federation of Small Businesses, 72% of small businesses in England and Wales experienced cybercrime in the last two years; 1.89 million experienced fraud in the same period, with the most common variants being invoice fraud, card fraud, and unauthorised payments.

Though small businesses have been taking steps to protect themselves – 93% have taken at least one cybersecurity measure, with 56% increasing investment in this area over the last two years – there's still a mixed picture.

Nearly three-quarters of small businesses detected cybercrime or fraud incidents within hours, but for 6% it took a week and 8% only identified the threat after a month. Government accredited cybersecurity measures, like Cyber Essentials, aren't cutting through; only 6% of small firms held this standard, an increase of just 4% since 2019.

Det Supt Kirby told Policing Insight that this is becoming all the more challenging, with cybercrime tools that are easier and easier to use. "Ransomware remains the biggest threat, but threats fluctuate and change. We have seen hugely complex cybercrime types – that used to only be delivered by high-end state actors, a really nice criminal set – now become widely available. They're often franchised and available so that even kids sat in their bedrooms can use free tools to launch devastating attacks or ransomware.

"Criminal tools have become more widely available. Cyber and fraud is hugely under-reported, even though reported fraud and cyber is already nearly 40% of all recorded crime; it would worry me what the true size and scale of that is."

And the cases Det Supt Kirby dealt with during his time as a cybercrime investigator illustrate the harm digital crime can cause. "There was this small, family-run legal aid firm connected to

the national legal aid network. They experienced a cyberattack, a brute force attack through an admin assistant's laptop which had a weak password.

"They gained access to the network, stole all their data and held it for ransom. The impact shows the risk. You might think it's just a small legal firm in the middle of nowhere, but the impact was risking 260,000 criminal cases which [were held on their devices]."

The company's victim impact statement – included in a presentation from a regional cyber resilience centre – shows how disorienting this kind of incident can be.

After suspicious activity was identified on the legal firm's servers, it was initially flagged as a "non-material breach" with no data leaving their network. However, the statement explains: "Later that evening, all staff received an email from the hackers responding to the email we had sent.

"The email was sent from one of our own staff member's email account. The email explained how data had been exfiltrated from our system and that all the data in our system had been encrypted."

Fortunately, the company had backed up its systems properly (meaning that the data could be restored) and none of the cases involved were live. But it shows how easy it is to fall victim to cybercrime – even if you are prepared.

"We have learnt the hard way that anyone can be a victim no matter how secure you think your infrastructure is," added the firm in its statement. "We have always had procedures in place to ensure that we're secure, such as regularly changing passwords, having up-to-date security software and backing up our server on a regular basis, yet we still fell victim to an attack."

Artificial intelligence

The other factor that could increase the cybercrime threat is artificial intelligence (AI). In a speech from October 2023, UK Security Minister Tom Tugendhat outlined this risk in stark terms, saying: "Unchecked, AI has the power to bring about a new age of crime." ChatGPT and other generative tools could make it easier than ever to commit fraud."

Det Supt Kirby argued that a tailored approach, adapting to the needs of small businesses, is the only way to deal with this threat. “I go to lots of conferences on AI, it’s a hot topic. But I don’t think anybody fully understands the threat it poses at the moment. Lots of people are talking about, you know, ‘we’re going to have robots walking down the street trying to kill us, and networks trying to take over the world’. I’m not sure that is the case and it’s so far removed from the sector of society we’re trying to help.

“AI might well speed up and enhance some of the ways we work – our intelligence picture, data analysis, and threat prediction. It may increase the vulnerability of SMEs. But the clients I speak to don’t care about all that, they care about their customer base, bringing money in the door, and being able to pay their expenses. That’s about the extent of their worry.

“If I start saying ‘AI is going to increase the threat to your business’, I’m going to lose their interest very quickly.

“I see my job and that of the regional network as being to interpret that threat and discuss it in layman’s terms, without scaring the bejesus out of the florist, plumber, or librarian that we’re talking to. That’s the level of client we’re dealing with.

“Your big companies like Amazon and Microsoft will put lots of time and money into AI research, but the little plumber’s merchant at the end of the high street isn’t going to care about that. That’s who I’m here to protect.”

A message to policing

Det Supt Kirby is only six months into his tenure as CEO of the NCRCG; but what are his long-term aspirations for the sector? What would the ideal state of play be in a decade’s time around cyber resilience?

“I would like the cyber resilience brand to be a recognised brand of policing, not just to the SMEs who we target at the moment, but to the wider public. Everybody should have a base understanding of how to protect themselves online, starting at the real basics of having a strong password and multifactor authentication. If everybody in the country knew that, my job is done and we’ll have helped to protect the UK economy.”

His view is that it's about policing doing what it has always done, but in a digital context. "When I first joined up, I went through my probation and learnt to be a good copper, we introduced things like victim support leaflets," continued Det Supt Kirby.

"Where there's a burglary in the road, you'd go and post some packs in the neighbouring addresses with a bit of advice: there's been a burglary in the area, maybe invest in an alarm, keep your windows shut at night, lock up your garage, check your front door lock is good enough. Simple advice that people can put in place.

"Move forward 20+ years into the cyber world I work in, it's no different. Every cop should be empowered to be out there going to cybercrime jobs, because we're in such a digitally connected world. Every cop should have the basic knowledge to go out there and support a victim – that basic advice: lock up your bike, get a burglar alarm, have a strong password on your phone, think about multifactor authentication. Nothing more complicated than that."

His message to the average police officer reading this, who might not ever have worked on cybercrime, is equally straightforward: "You don't have to go into the deep dark depths of cryptography or anything. You just need to be able to give basic cybercrime advice like you have always done.

"And offer all that advice in addition to saying: 'Have you heard of your local cyber resilience centre? They can support you.' It's just basic crime prevention. It's just policing in the modern world."

Read the first part of the interview

Det Supt Ian Kirby: 'Working in cybercrime, I've helped more people than in the rest of my career'

After his first six months leading the National Cyber Resilience Centre Group – a not-for-profit partnership that enhances the cyber resilience of small businesses – Detective Superintendent Ian Kirby has ambitious plans for growth and a call to arms for police officers around cyber prevention, as Policing Insight's James Sweetland reports.

Picture © Thapana_Studio / Shutterstock

This article can be found here:

Det Supt Ian Kirby: ‘Every cop should have the basic knowledge to go out there and support a victim’

© Policing Insight 2024. Reprinted by subscriber: Ian Kirby for use by National Cyber Resilience Centre Group (NCRCG) only 8 of 8